(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 1 161 055 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
05.12.2001 Bulletin 2001/49

(51) Int Cl.[7]: **H04L 29/06**

(21) Application number: **01480006.4**

(22) Date of filing: **23.01.2001**

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE TR
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: **29.02.2000 EP 00480024**

(71) Applicant: **INTERNATIONAL BUSINESS MACHINES CORPORATION**
Armonk, NY 10504 (US)

(72) Inventor: **Fiammante, Marc**
06700 St Laurent du Var (FR)

(74) Representative: **Etorre, Yves Nicolas**
Compagnie IBM France,
Département Propriété Intellectuelle
06610 La Gaude (FR)

(54) System and method of associating devices to secure commercial transactions performed over the internet

(57) The invention discloses how to associate communications devices so as to carry out secure transactions over an untrusted network i.e., the Internet. The communications devices are assumed to be independently capable of communicating with an electronic commercial-like site managing a directory of legitimate users which all possess a token e.g., a chip-card. Then, whenever one user desires to carry out a secure transaction it first prepares it from a communications device featuring convenient interfaces e.g., a personal computer with large display and keyboard. When done, signature of the secure transaction must be obtained from another communications device through which the legitimate user is reachable and which is enabled with the token it possesses. When called from the commercial-like site the second communications device can thus, check, sign and transmit back to the commercial-like site the signed secure transaction where its final processing can go on. Therefore, the invention combines built-in features of standard communications devices to conveniently carry through elaborated secure transactions that would otherwise require added features such as large displays and keyboards to wireless mobile devices or chip-card reader to personal computers.

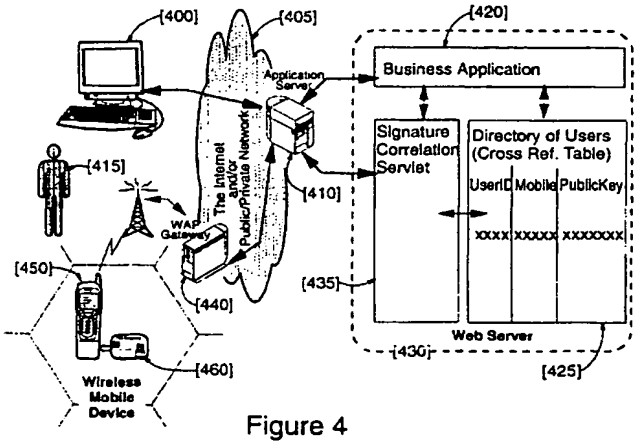

Figure 4

EP 1 161 055 A2

Description

Field of the Invention

[0001] The present invention relates generally to the Internet and more particularly applies to electronic commerce and to commercial-like transactions that take place over the Internet requiring that originator of such a transaction should neither be able to masquerade as someone else (originator must be authenticated) nor can later deny to have actually effected the transaction (non-repudiation).

Background of the Invention

[0002] Commerce over the Internet is dramatically expanding. It involves all sorts of transactions implying the movement of electronic money. All of this is taking place over what is, basically, a very unsecured network. Therefore, based on cryptography, numerous techniques and methods have been devised not only ensuring confidentiality of the transactions but also, this is often even more important, authentication, integrity and non-repudiation. Authentication is required to ascertain the origin of a transaction so as no one should be able to masquerade as someone else. Integrity is key to make sure that a transaction has not been modified, unintentionally or maliciously, on its way through the network to destination e.g., a server aimed at processing the customer orders. Finally, non repudiation is essential to make sure that a completed transaction, that may involve a lot of money, may not just be denied later on by any of the participants.

[0003] Accessing the Internet is mainly achieved nowadays from a PC (Personal Computer), a WS (Work Station) or any computer-like device capable of running a piece of software, referred to as a browser, in order to be able to get on the World-Wide Web (or just the Web) the ubiquitous application that has accompanied the explosive growth of the Internet in past years. Thus, an Internet commerce site is a particular Web site aimed at handling commercial transactions. A well-known site is e.g., located at http://www.amazon.com/. It is a huge virtual bookstore selling also music and videos. They claim that millions of people, from many countries, have indeed made online shopping on their site. Although such sites also claim they are completely safe (since one has to disclose them a credit card number to buy something) they actually fail meeting satisfactorily all of the criterions here above mentioned that is, authentication, integrity and non-repudiation. To reach completely these objectives connecting PC's would need to be equipped with smart card readers and users would have to carry a token i.e., intelligent chip-cards or smart-cards so that authentication based on the knowledge (PIN or password) and possession (card) principle can be carried out. Smart-cards are also suitable for storing certificates and encryption keys securely. Smart cards with an integrated crypto-processor can implement cryptographic functions directly on the card so that the keys never leave the smart card. For example, a digital signature, which generally consists in encrypting, with user private key, a digest obtained through the application of a hash function over transaction content then, appended to it so that recipient may later check the transaction with user public key and make sure that it has not been altered on its way and has well been originated by whom possesses the corresponding private key. This eliminates any possibility of the key falling into the wrong hands. However, all of this is only possible is PC is indeed equipped with the proper hardware i.e., a card reader and the corresponding software or device driver to perform the adaptation with the OS (Operating System) running on the PC. This is a new technology and a new type of I/O port to be added to PC's. This has a cost which does not fit well with the general trend that wants to reduce as much as possible the operational expenses of a private or enterprise network hence, requiring to lower the cost of terminal equipment's and TCO (Total Cost of Ownership). Thus, in practice, when manufactured, PC's are still seldom equipped with such card readers. Although a separate chip card reader can always be later added to a particular PC this requires that the corresponding software, the device driver, be also installed thus further personalizing it.

[0004] On the other hand another even more explosive market is the one of mobile wireless communications first mainly driven by mobile digital cellular phones however, rapidly evolving to cover other applications in relation with the Internet such as e-mail in a first place. It is anticipated that electronic commerce applications such as personal banking, stock trading, gambling, ticket reservations and shopping will soon become commonly available on mobile phones. Hence, the security of data communications over wireless networks has become a major concern to mobile commerce businesses and users which has triggered the development of products to build secure systems that solve the core requirements of electronic commerce security already here above mentioned namely: confidentiality, authentication, integrity and non-repudiation. Also, standards are being put in place to control the development of such products and make sure that they may inter operate. The Wireless Application Protocol (WAP) Forum (http://www.wapforum.org) has thus become the de facto worldwide standard for providing Internet communications and advanced telephony services on digital mobile phones, pagers, personal digital assistants and other wireless terminals. Therefore, all these devices, contrary to PC's, are promised to be upfront equipped with all necessary features and functions so as to guarantee security of electronic commerce transactions. Nevertheless, they all also have inherent limited display capability and rudimentary user interface along with limited processing power, battery life and storage capabilities.

[0005] Therefore it is a broad object of the invention

to combine the advantages of PC's which have great display and user interface capabilities with the built-in security features of modern wireless mobile devices so as to enable convenient and secure electronic commerce transactions.

[0006] Further objects, features and advantages of the present invention will become apparent to the ones skilled in the art upon examination of the following description in reference to the accompanying drawings. It is intended that any additional advantages be incorporated herein.

Summary of the Invention

[0007] A method and a system of associating communications devices to carry out a secure transaction over an untrusted network from an electronic commercial-like site are disclosed. The communications devices are independently capable of communicating with the electronic commercial-like site which manages a directory of legitimate users each having an identification record. The users are also assumed to possess a token e.g., a chip-card. Then, whenever one legitimate user desires to carry out a secure transaction this latter is first prepared with the help of a first communications device, featuring convenient human being interfaces e.g., a personal computer. When done, an approval of the secure transaction content is forwarded to the commercial-like site, from the first communications device. When the approval is received in the commercial-like site the identification of a second communications device, through which the legitimate user is reachable, is retrieved from its identification record. This triggers the issuing of a request, from the commercial-like server towards the second communications device, to have the secure transaction signed. Hence, signature of the secure transaction is carried out with the second communications device, enabled by the token of the legitimate user thus, obtaining a signed secure transaction which is transmitted back to the commercial-like site which performs a final checking in order to complete the secure transaction.

[0008] Therefore, the method and system of the invention combine built-in features of standard communications devices to conveniently carry out secure commercial-like transactions over an intrusted network i.e., the Internet. Especially, the invention neither requires that standard personal computers or work station be equipped with a chip-card reader nor that wireless mobile devices need to have large displays and keyboards to be able to carry through elaborated transactions.

Brief Description of the Drawings

[0009]

Figure 1 depicts the state of the art where the Internet can be accessed independently either from a personal computer or a wireless mobile device.

Figure 2 is an example of a commercial transaction, per the invention, in which a personal computer and a wireless mobile device cooperate to carry it out.

Figure 3 shows an example of the correlation table, according to the invention, cross referencing the transaction identifiers that permits to perform a secure transaction.

Figure 4 illustrates the overall architecture of the system through an example involving a personal computer and a cellular mobile phone.

Detailed Description of the Preferred Embodiment

[0010] **Figure 1** illustrates current art where a user [100] may have access to a commercial Internet Web site e.g., the AMAZON.COM virtual bookstore [105] (at http://www.amazon.com) to perform a transaction such as buying a book. This can be done e.g., from a personal computer (PC) [110] having a connection to the Internet [115] through a modem or a LAN (local area network) and running a browser capable of conveniently displaying pages from the here above Web site so as user [100] can gather all necessary information on what it is buying. Current PC's are always equipped with large display monitors [120] having at least a 15-inch wide screen (diagonal) capable of displaying 800x600 pixels or more. PC's are also always equipped with a 100-key+ keyboard [125] and a pointing device, usually a mouse [130]. The same user [100] is also commonly carrying a mobile telephone [140] or any equivalent wireless portable device which are now able to connect to the Internet too [145]. Moreover, they are personalized with a token e.g., a smart-card or chip-card [155] so as user [100] may be uniquely identified. However, contrary to PC's, those wireless portable devices have very poor display capabilities [160], limited to a few lines of a few characters, and have rudimentary numeric keyboards [150].

[0011] **Figure 2** depicts a typical transaction according to the invention, involving a client PC machine [200] (or a work station or any computer-like device) and a wireless portable mobile device [210] e.g., a mobile phone. Transaction is initiated from the client PC at step [201] when a user, having access to this PC, must reach a remote server, typically through the Internet or through any public and/or private network or combination of, on which a business application [230] is running setting up the commercial-like site user desires to deal with. In the example chosen in figure 1 this is the amazon.com virtual bookstore. Then, the first action from the application is to request [231] client authentication. User responds

to the request complying with whatever method is in effect in the server i.e., provides credentials to be recognized as a legitimate user. The standard practice is to send [202] a user ID with a password. More sophisticated methods might also require the sending, by the client and/or the server, of certificates issued by a third party i.e., a CA (Certificate Authority), trusted by user and/or server. Irrespective of the method enforced in the server, when satisfied, this latter eventually authenticates the user [232] unless (this is not shown) user fails answering satisfactorily in which case the transaction is obviously aborted by the server. All of this can actually be implemented from various well known methods known by those skilled in the art. Many variants exist. As an example, certificates could be X.509 certificates as described in RFC2459 of the IETF (Request For Comments of the Internet Engineering Task Force) used by the Web browsers supporting SSL (Secure Socket Layer) protocol which is being standardized under the name of TLS (Transport Layer Security) protocol in RFC2246. As far as Web server is concerned the only other assumption is that it is capable of generating static and dynamic HTML (Hyper Text Markup Language) pages, the language of the Web, that are thus view able from the Web browser client machine [200].

[0012] When the user has been recognized as a legitimate user by the server it is then permitted to browse the server HTML pages of the application so as to gather all the necessary information regarding the transaction user wants to perform. This assumes that multiple exchanges may have to take place between the client machine [203] and the server [233] and generally require that users fill virtual forms [204] i.e., dynamic HTML pages formatted by the server [234], that this latter will use to interpret the content of the transaction so as to determine what user intends to do. In the previous simple example of the amazon.com server, a virtual shopping cart is filled e.g., with book(s) that the user desire to acquire. While filling its cart a user has thus, optionally, the possibility of consulting all the information provided by the server about the books, their authors, the press critics along with their prices, availability, delivery options and generally all sorts of data that a customer is willing to know before proceeding to a virtual cash register.

[0013] Thus, when the user is finally satisfied with the content of the transaction thus, having completed the overall preparation phase [240] it eventually approves it [205] from the client PC. Still referring to the here above example of the amazon.com bookstore this occurs when it has finished filling its virtual shopping cart. In another example this is because user has finalized its today list of shares he wants to sell or buy through the server of its preferred broker. Obviously, although not explicitly shown, user has always the freedom of aborting the transaction any time before completion. Or, the transaction may be aborted just because something wrong happens between the client PC and the server such as an interruption of the communication. However, normally, the transaction is approved by the user from the client PC [205]. At this point, in most of today's commercial Web site, the essential of the transaction is over if one excepts the sending by the server of a closing message confirming the terms and content of the transaction also thanking the user that is, the Web site customer. However, all of this rests on the good faith of both parties. The owner of the commercial Web site might not sent the ordered items. The user might use a fake or stolen credit card number or it may later deny to have really effected the transaction. To overcome this, methods have been devised so as none of the parties involved can masquerade as someone else nor may later deny to have effected the transaction. However, this requires some form of strong authentication and electronic signature that the user side may only fulfilled if the client PC is indeed equipped with the proper equipment that is, a smart-card reader and its related supporting software or 'driver', so as the user of the client PC may prove it is the one it pretends to be through the possession of a token i.e., its smart-cart. However, standard PCs and working stations are seldom equipped nowadays with such a piece of hardware and there is no clear sign that this will become a standard feature (like a mouse) in a foreseeable future even though, it is obviously always possible to add, on a particular PC, a separate card reader and install the proper software to drive it.

[0014] On the other hand, while Internet and the electronic commerce was dramatically growing, an even more explosive market is the one of the wireless mobile devices; first of all, cellular mobile phones, which have been universally accepted. Because the latest versions of these devices are now able to connect to the Internet too and also, because their use is conditioned to the insertion of a smart-card, so that the bearer is identified, they become the device of choice to perform strong authentication and to approve and sign commercial transactions. Therefore, the method of the invention assumes that the user of the client PC, that has initiated the transaction, is also carrying such a wireless mobile portable device. Then, transaction goes on with step [235] when Web server needs to obtain the signature of it by the user. To do so, server manages at least one table, an example of which is further described in figure 3, cross-referencing all legitimate user IDs that are permitted to access the Web site along with their mobile device ID and public key (held in the user own token e. g., a smart-card). Hence, table is looked-up to retrieve user phone number and smartcard public key. After which, the transaction data are formatted and optionally signed [236] using the user smart-card public key also, optionally, further countersigned with the server private key (so as user is made certain of the origin of the transaction if necessary) and the Web server dials automatically the user mobile phone [221], using WTA standard previously discussed, providing for mechanisms that allow origin servers to deliver data to a mobile terminal even though this latter has not issued any request.

Meanwhile, Web server holds PC Web request [222] until mobile device eventually responds. This part of the signature process, in which business application is issuing the signature request [250], is shown to be implemented here mainly under the form of a so-called Java™ Servlet [220]. While Java™ is, among other things, a popular, simple, object-oriented, distributed and interpreted general-purpose programming language developed by Sun Microsystems (Sun Microsystems, Inc., 901 San Antonio Road, Palo Alto, CA 94303 USA.) Java™ Servlets are small, platform-independent Java™ programs that can be used to extend the functionality of a Web server in a variety of ways thus, are convenient to implement the signing function of the invention. However, this is only one example of carrying out the invention. The ones skilled in the art will recognize that, without departing from the spirit of the invention, it may be implemented in many alternate equivalent ways. Especially, the signing process could be imbedded into the Web Server application so as the two processes [220] and [230] are merged. When user accepts the incoming call on his mobile device, Web generated transaction content, optionally signed with user public key and possibly countersigned with server private key, may be checked by the smartcard if it is necessary to ascertain its origin [211]. Then, user is prompted to validate the transaction. At this point user may want to review the content of the transaction [212] received on its mobile wireless device (which is sufficient in general to be sure what transaction is being signed). Transaction may be displayed on the mobile screen, preferably in an abridged form for the sake of convenience, due to the limited capacity of the display of such devices. Alternatively, this step may just be replaced by the display of a number, associated with the transaction, a common practice when dealing with a Web server or ordering goods or services over the phone. This transaction number may thus be used as a correlator so as user is made certain of what transaction is being validated. After this, smart-card is requesting a PIN (personal identification code) [213] so as transaction can now be signed with user private key [214]. Using a PIN to enable this operation is standard practice with current smartcards. More sophisticated methods are soon to be widely available. These methods have In common to use biometric data e.g., the finger prints of the user are recognized through an appropriate sensor placed on the smart-card. This will add definitively to the security hence, better contributing to reach the goals of the invention i.e., authentication, integrity and non-repudiation of commercial transactions from standard widely available devices. At this point the overall process [260] to carry out signature of the secure transaction in user mobile device is over. Then, next step [215] consists in sending back to the server the signed transaction (signed with user private key). Business application running on server thus, completes the signature cycle in a global checking step [270] including a completion step [223] for signing servlet [220], a checking step in server [237] utilizing user public key followed by the sending [238] of a last transaction status, under the form of a new Web page, to the client PC machine at the origin of the transaction.

[0015] **Figure 3** illustrates a preferred embodiment of the cross-referencing table or directory mentioned in figure 2 and required to carry out the invention. Table [300] lists the users [310] that are recognized by the Web server as being legitimate users authorized to deal with the business application. For each registered user, a mobile device ID number to call i.e., a phone number [320], is first listed. Secondly, the public key [330], corresponding to the token (smart-card) of the user, is recorded too so that server holds, in an identification record [340], for every user, all necessary information to carry out secure commercial transactions. The precise form under which table is actually implemented and the way it is searched when interrogated is beyond the scope of the invention. Those skilled in the art will recognize that numerous alternate ways e.g., tailored to favor performance or memory size required, are feasible. As an example table could be implemented to obey the specifications of LDAP (Lightweight Directory Access Protocol) a protocol for accessing on-line directory services defined by the IETF (Internet Engineering Task Force) in RFC's (Request For Comments) especially, RFC 1777. LDAP defines a relatively simple protocol for updating and searching directories running over TCP/IP (the Internet suite of protocols). An LDAP directory entry is a collection of attributes with a name, called a distinguished name (DN). The DN refers to the entry unambiguously. Each of the entry's attributes has a type and one or more values. The types are typically mnemonic strings, like "cn" for common name, or "mail" for e-mail address. LDAP directory entries are arranged in a hierarchical structure that reflects political, geographic, and/or organizational boundaries. Entries representing countries appear at the top of the tree. Below them are entries representing states or national organizations. Below them might be entries representing people, organizational units, printers, documents, or just about anything else. Therefore, cross-referencing table of the invention can advantageously be implemented under the form of a customized LDAP directory.

[0016] **Figure 4** shows all the components of the system per the invention. It involves a standard PC [400] or any computer-like machine capable of accessing, over the Internet or any combination of public/private networks [405], a server [410] running the application i.e., a business application [420] core of a commercial-like site [430] that user [415] wants to deal with. Then, initial part of the transaction is thus conducted from the PC [400]. When user is satisfied with contents and objects of the transaction it approves it. This enables the corresponding part of the business application [435] running over the server [410] and using one or more directory or cross-referencing table [425] aimed at logging the us-

ers permitted to access the business application, to trigger the sending of a signature request towards user's wireless mobile device e.g., its cellular mobile phone [450]. This is done through the network [405] and a wireless gateway [440] operated e.g., according to the Wireless Application Protocol (WAP). Hence, transaction may be approved from the token [460] that user possesses (usually a smart-card) housing, among other things, its private key, in order to complete the transaction in signing it therefore, allowing to meet all the goals of a secure transaction namely, strong authentication, integrity and non-repudiation.

Claims

1. A method of associating communications devices [400] [450] to carry out a secure transaction over an untrusted network [405] from an electronic commercial-like site [430], said communications devices independently capable of communicating with said electronic commercial-like site, said electronic commercial-like site managing a directory [425] of legitimate users [415] each having an identification record [340], said legitimate users each possessing a token [460], said method comprising the steps of:

   when ever one of said legitimate users [415] desires to carry out a said secure transaction:
   preparing [240] said secure transaction from a first said communications device [400] featuring convenient human being interfaces [110] [120] [130] to communicate with said commercial-like site [430];
   when done:
   forwarding to said commercial-like site, from said first communications device, an approval [205] of content of said secure transaction;
   when said approval is received in said commercial-like site for said secure transaction prepared by said legitimate user:

      retrieving [235] in said identification record [340] of said legitimate user an identification of a second communications device [320] through which said legitimate user is reachable;

      issuing [250] in said commercial-like server towards said second communications device a request to have said secure transaction signed;

      carrying out signature [260] of said secure transaction from said second communications device enabled with said token of said legitimate user thus obtaining a signed secure transaction;

      transmitting [215] said signed secure transaction back to said commercial-like site;

      checking [270] in said commercial-like site said signed secure transaction;

   thereby, completing said secure transaction.

2. The method according to claim 1 wherein each said identification record [340] of said directory [300] in said commercial-like site includes:

   a user identification [310] of a said legitimate user;

   a device identification [320] of a said second communications device through which said legitimate user is reachable;

   a user public key [330] contained in a said token owned by said legitimate user.

3. The method according to any one of the previous claims wherein said token [460] of said legitimate user includes the storing of:

   a user private key;

   a personal identification number (PIN).

4. The method according to any one of the previous claims wherein said preparing step includes the steps of:

   accessing [201] a Web server business application [230] in said electronic commercial-like site [430];

   providing, in response to a request for authentication [231] from said Web server business application, credentials [202] to be recognized as a legitimate user [232];

   browsing [203] [233] said electronic commercial-like site;

   filling in [204] [234] all required information to allow completion of said commercial-like transaction.

5. The method according to any one of the previous claims wherein said issuing step [250] includes the steps of:

   formatting [236], in said commercial-like site, a request to have said secure transaction signed in said second communications device, said

step of formatting a request optionally including the further steps of:

signing origin of said request, said step of signing origin including:

employing said user public key of said legitimate user;

additionally employing a private key of said commercial-like site;

forwarding [221], from said commercial-like site, to said second communications device said request;

waiting [222] till said second communications responds.

6. The method according to any one of the previous claims wherein said step of carrying out signature [260], in said second communications device, includes the steps of:

checking [211] said request to have said secure transaction signed, said step of checking optionally including the further step of:

authenticating origin of said request;

displaying [212] content of said secure transaction;

prompting [213] said legitimate user to enter said PIN of said token; signing [214] said request with said user private key.

7. The method according to claim 6 wherein said step of prompting [213] said legitimate user to enter said PIN is replaced by the step of analyzing biometric data of said legitimate user.

8. The method according to any one of the previous claims wherein said checking step [260], in said commercial-like site, includes the steps of:

detecting [223] completion of signature by said second communications device;

checking [237] said signed request transaction with said public key of said legitimate user;

forwarding [238] a transaction status to said first communications device.

9. The method according to any one of the previous claims wherein said first communications device is a standard personal computer.

10. The method according to any one of the previous claims wherein said second communications device is a token enabled wireless mobile device.

11. A system, in particular a server implementing a commercial-like site, comprising means adapted for carrying out the method according to any one of the previous claims.

12. A computer-like readable medium comprising instructions for carrying out the method according to any one of the claims 1 to 10.

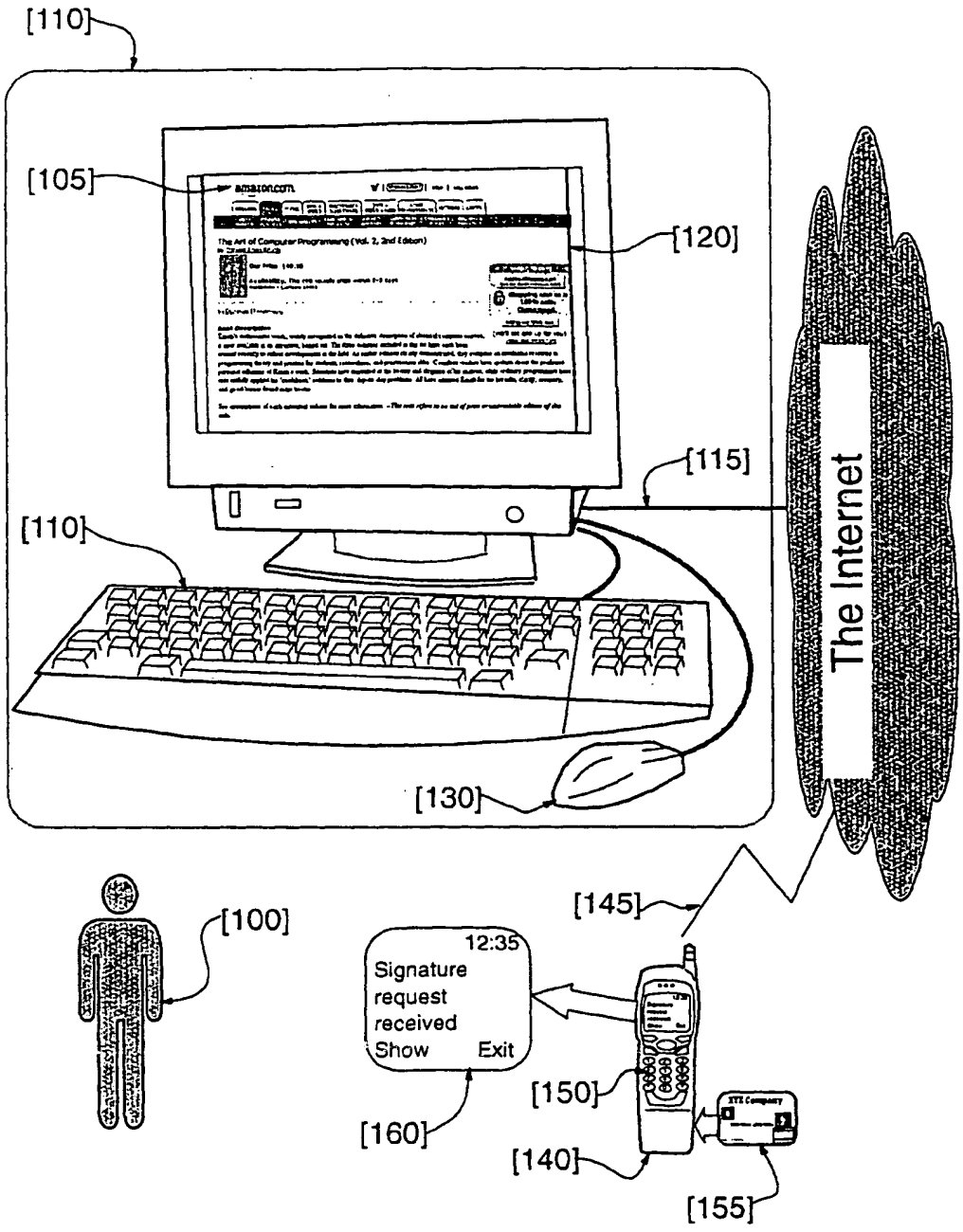
[110]
[105]
[120]
[115]
[110]
[130]
The Internet
[145]
[100]
12:35
Signature
request
received
Show
Exit
[150]
[160]
[140]
[155]

Figure 1

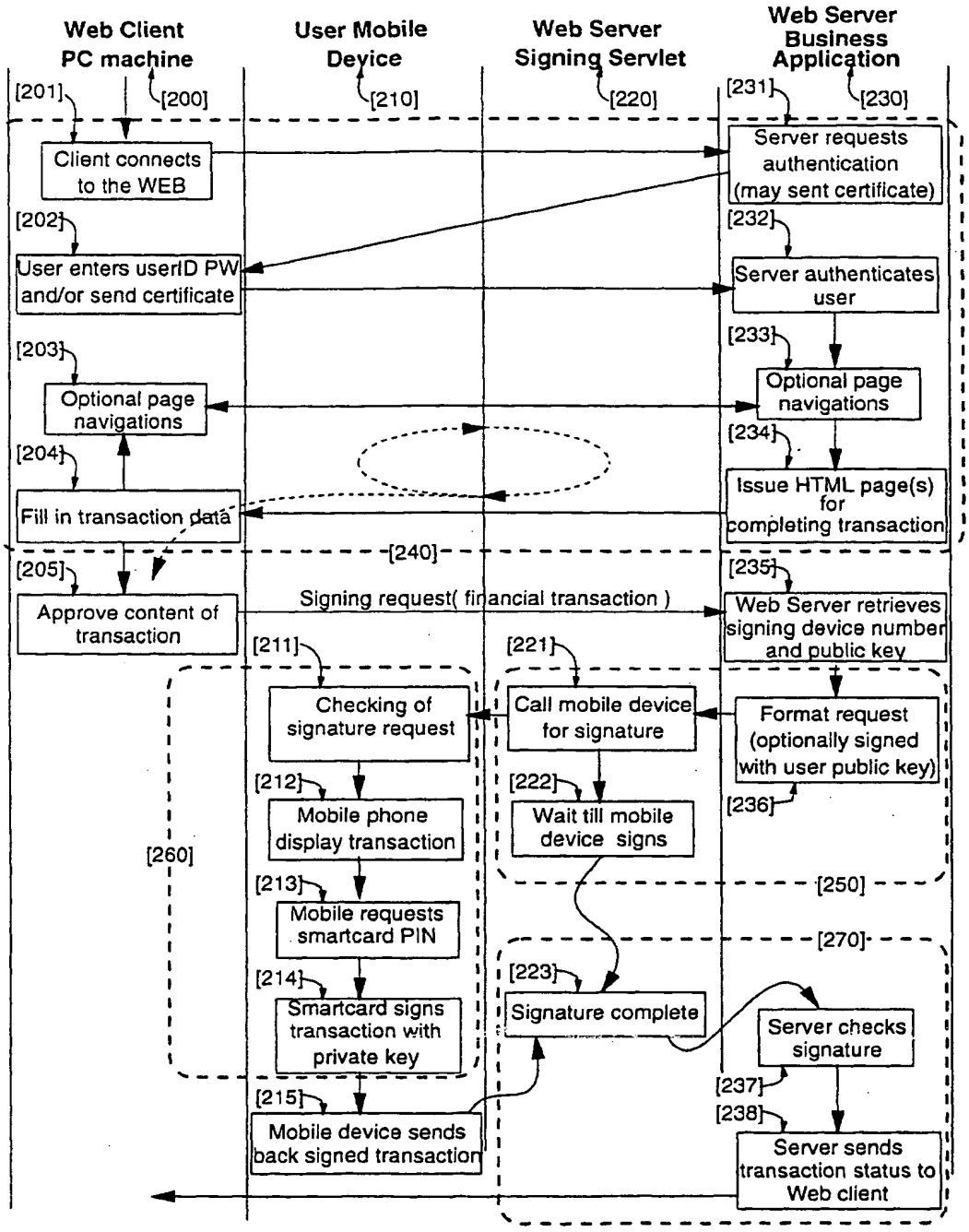
Web Client PC machine
User Mobile Device
Web Server Signing Servlet
Web Server Business Application
[201]
[200]
[210]
[220]
[231]
[230]
Client connects to the WEB
Server requests authentication (may sent certificate)
[202]
[232]
User enters userID PW and/or send certificate
Server authenticates user
[233]
[203]
Optional page navigations
Optional page navigations
[234]
[204]
Issue HTML page(s) for completing transaction
Fill in transaction data
[240]
[205]
[235]
Approve content of transaction
Signing request(financial transaction)
Web Server retrieves signing device number and public key
[211]
[221]
Checking of signature request
Call mobile device for signature
Format request (optionally signed with user public key)
[212]
[222]
[236]
Mobile phone display transaction
Wait till mobile device signs
[260]
[250]
[213]
Mobile requests smartcard PIN
[270]
[214]
[223]
Smartcard signs transaction with private key
Signature complete
Server checks signature
[237]
[215]
[238]
Mobile device sends back signed transaction
Server sends transaction status to Web client

Figure 2

[300]

UserID	Mobile Device ID	User Public Key
User#0001	+33612345672	0300460218BEFC1A4E3 D4D617263204696
User#0002	+33676543211	40A4B603G00302004F5 53D4672616E63
User#nnnn	+33614289024	3A6525G0024FG002024 FG00204B44700

[340] [310] [320] [330]

Figure 3

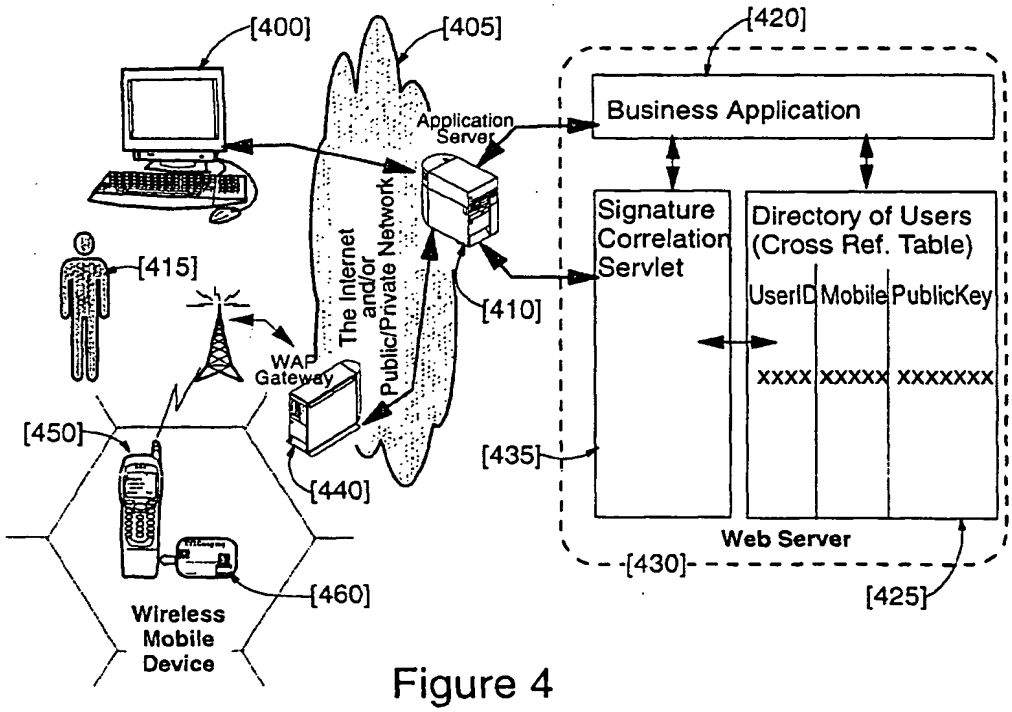

Figure 4